Hacking y Pentesting con Python

Módulo 2: Fingerprinting y Banner grabbing.

eip ESCUELA INTERNACIONAL POSGRADOS

Fingerprinting y Banner grabbing.

ACTIVIDAD MODULO 2

Objetivos

- Instalar las librerías necesarias para integrar scripts en Python con Metasploit Framework.
- Familiarizarse con la creación de scripts para integrar Python con Metasploit Framework.
- Aprender a utilizar Metasploit Framework desde scripts desarrollados en Python.
- Aprender a invocar los diferentes tipos de componentes disponibles en Metasploit Framework para labores de pentesting.

Contenido correspondiente a módulo 2:

1. Configurar el entorno de trabajo con Metasploitable 2 y Kali Linux.
2. Realizar pruebas entre ambos sistemas con el objetivo de comprobar su correcto funcionamiento. Es importante hacer esto antes de empezar la práctica y ejecutar las rutinas en Python.

Actividad relacionada con la lección 2:

1. Descargar e instalar Metasploitable2 y Kali Linux en VirtualBox. Realizar el proceso de configuración necesario para que ambas máquinas virtuales se puedan conectar. Se recomienda establecer la configuración de red en “modo puente” o crear una red “modo anfitrión” para ambos sistemas.
2. En la máquina Kali, crear un script en Python que sea capaz de integrarse con Metasploit Framework y explotar al menos 3 de las vulnerabilidades disponibles en Metasploitable2 de forma automática. Para ello, se debe usar la librería pymetasploit3 y levantar el servicio MSGRPC tal como se explica en la documentación.